FIG. 1

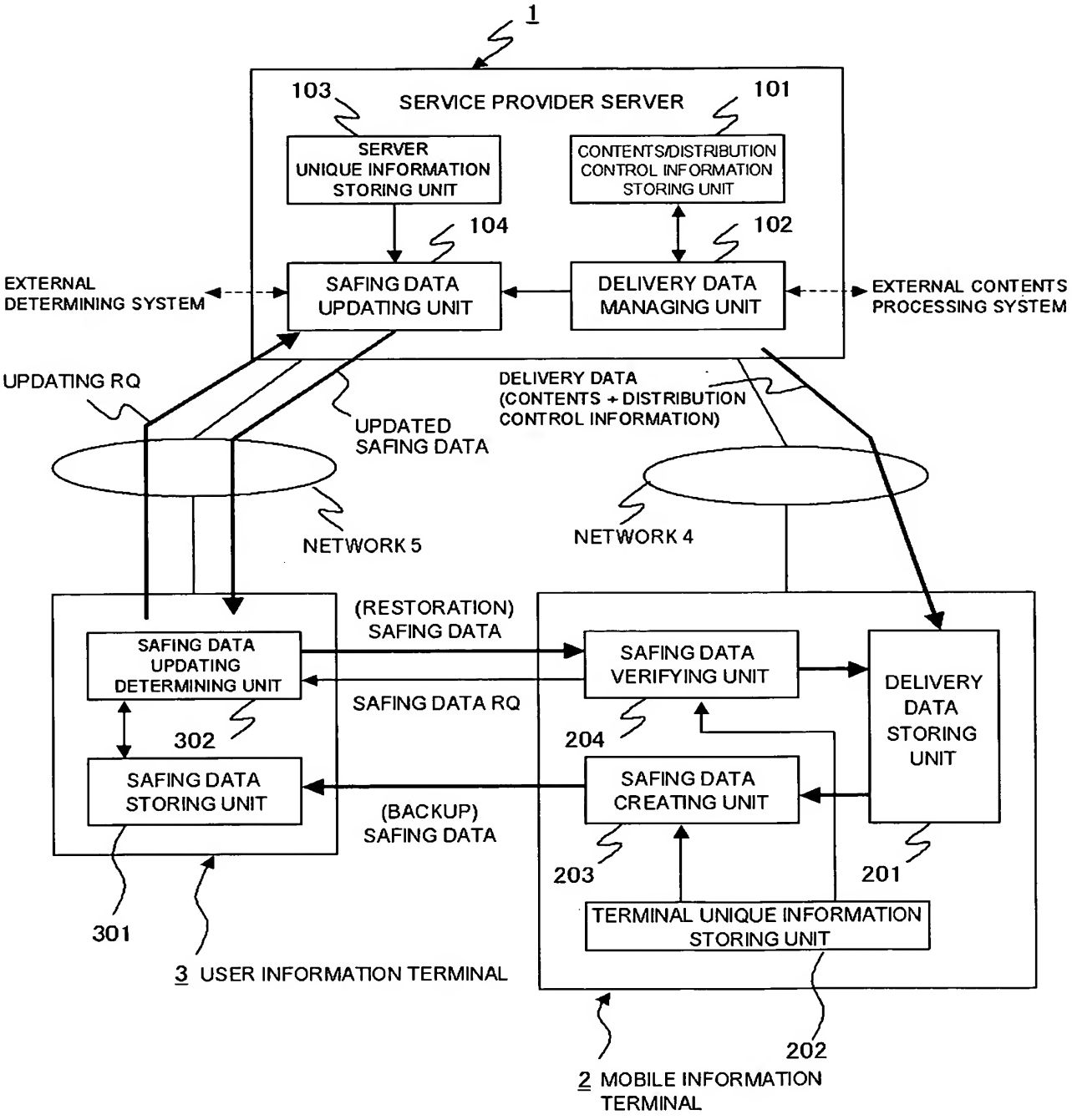

1
103
SERVICE PROVIDER SERVER
101
SERVER UNIQUE INFORMATION STORING UNIT
CONTENTS/DISTRIBUTION CONTROL INFORMATION STORING UNIT
104
102
EXTERNAL DETERMINING SYSTEM
SAFING DATA UPDATING UNIT
DELIVERY DATA MANAGING UNIT
EXTERNAL CONTENTS PROCESSING SYSTEM
UPDATING RQ
UPDATED SAFING DATA
DELIVERY DATA (CONTENTS + DISTRIBUTION CONTROL INFORMATION)
NETWORK 5
NETWORK 4
(RESTORATION) SAFING DATA
SAFING DATA UPDATING DETERMINING UNIT
SAFING DATA VERIFYING UNIT
DELIVERY DATA STORING UNIT
SAFING DATA RQ
302
204
SAFING DATA STORING UNIT
SAFING DATA CREATING UNIT
(BACKUP) SAFING DATA
203
201
TERMINAL UNIQUE INFORMATION STORING UNIT
301
3 USER INFORMATION TERMINAL
202
2 MOBILE INFORMATION TERMINAL

FIG. 2

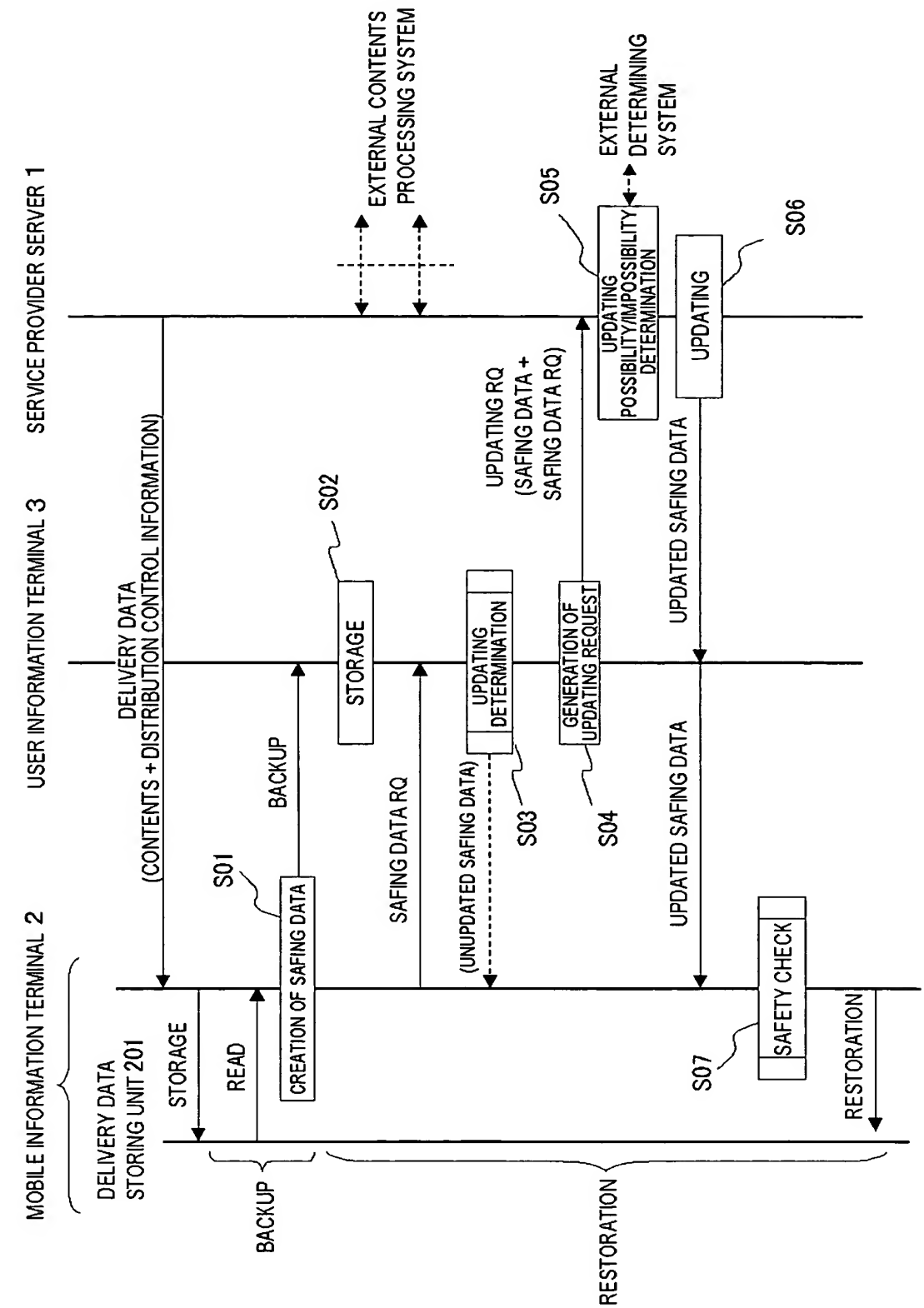
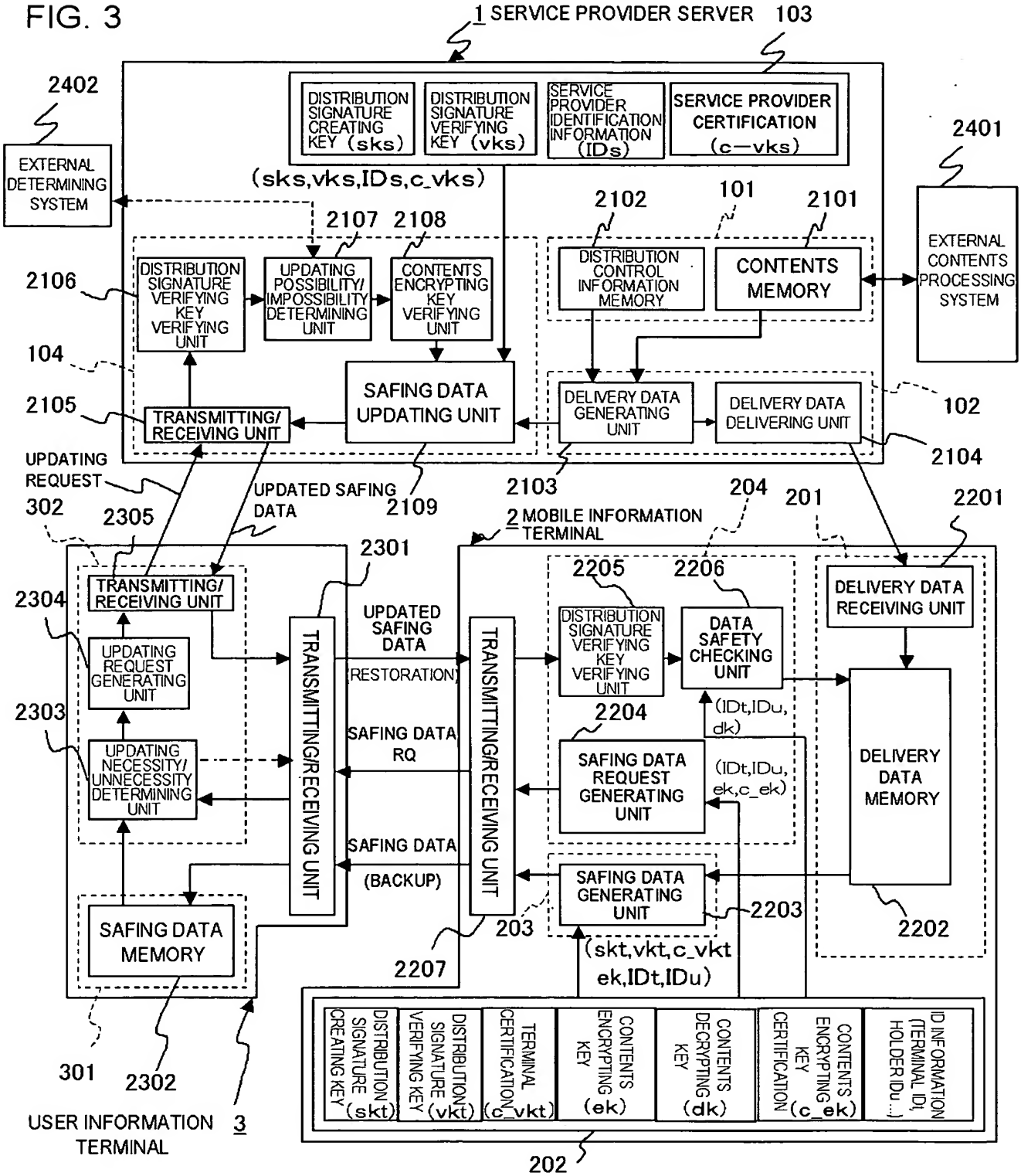

MOBILE INFORMATION TERMINAL 2
USER INFORMATION TERMINAL 3
SERVICE PROVIDER SERVER 1
EXTERNAL CONTENTS PROCESSING SYSTEM
EXTERNAL DETERMINING SYSTEM
DELIVERY DATA STORING UNIT 201
DELIVERY DATA (CONTENTS + DISTRIBUTION CONTROL INFORMATION)
S01
CREATION OF SAFING DATA
BACKUP
S02
STORAGE
SAFING DATA RQ
UPDATING DETERMINATION
(UNUPDATED SAFING DATA)
S03
GENERATION OF UPDATING REQUEST
S04
UPDATING RQ (SAFING DATA + SAFING DATA RQ)
S05
UPDATING POSSIBILITY/IMPOSSIBILITY DETERMINATION
S06
UPDATING
UPDATED SAFING DATA
UPDATED SAFING DATA
S07
SAFETY CHECK
STORAGE
READ
RESTORATION
BACKUP
RESTORATION

FIG. 3


1 SERVICE PROVIDER SERVER
103
DISTRIBUTION SIGNATURE CREATING KEY (sks)
DISTRIBUTION SIGNATURE VERIFYING KEY (vks)
SERVICE PROVIDER IDENTIFICATION INFORMATION (IDs)
SERVICE PROVIDER CERTIFICATION (c—vks)
(sks,vks,IDs,c_vks)
2402
EXTERNAL DETERMINING SYSTEM
2401
EXTERNAL CONTENTS PROCESSING SYSTEM
2102
101
2101
2107
2108
2106
DISTRIBUTION SIGNATURE VERIFYING KEY VERIFYING UNIT
UPDATING POSSIBILITY/ IMPOSSIBILITY DETERMINING UNIT
CONTENTS ENCRYPTING KEY VERIFYING UNIT
DISTRIBUTION CONTROL INFORMATION MEMORY
CONTENTS MEMORY
104
2105
TRANSMITTING/ RECEIVING UNIT
SAFING DATA UPDATING UNIT
DELIVERY DATA GENERATING UNIT
DELIVERY DATA DELIVERING UNIT
102
2104
UPDATING REQUEST
UPDATED SAFING DATA
2109
2103
204
201
2201
302
2305
2 MOBILE INFORMATION TERMINAL
2301
2205
2206
2304
TRANSMITTING/ RECEIVING UNIT
UPDATED SAFING DATA
DISTRIBUTION SIGNATURE VERIFYING KEY VERIFYING UNIT
DATA SAFETY CHECKING UNIT
DELIVERY DATA RECEIVING UNIT
UPDATING REQUEST GENERATING UNIT
TRANSMITTING/RECEIVING UNIT
(RESTORATION)
TRANSMITTING/RECEIVING UNIT
2303
2204
(IDt,IDu, dk)
UPDATING NECESSITY/ UNNECESSITY DETERMINING UNIT
SAFING DATA RQ
SAFING DATA REQUEST GENERATING UNIT
(IDt,IDu, ek,c_ek)
DELIVERY DATA MEMORY
SAFING DATA (BACKUP)
SAFING DATA GENERATING UNIT
2203
2202
SAFING DATA MEMORY
203
2207
(skt,vkt,c_vkt ek,IDt,IDu)
DISTRIBUTION SIGNATURE CREATING KEY (skt)
DISTRIBUTION SIGNATURE VERIFYING KEY (vkt)
TERMINAL CERTIFICATION (c_vkt)
CONTENTS ENCRYPTING KEY (ek)
CONTENTS DECRYPTING KEY (dk)
CONTENTS ENCRYPTING KEY CERTIFICATION (c_ek)
ID INFORMATION (TERMINAL IDt, HOLDER IDu ...)
301
2302
USER INFORMATION TERMINAL 3
202

10/536068

FIG. 4

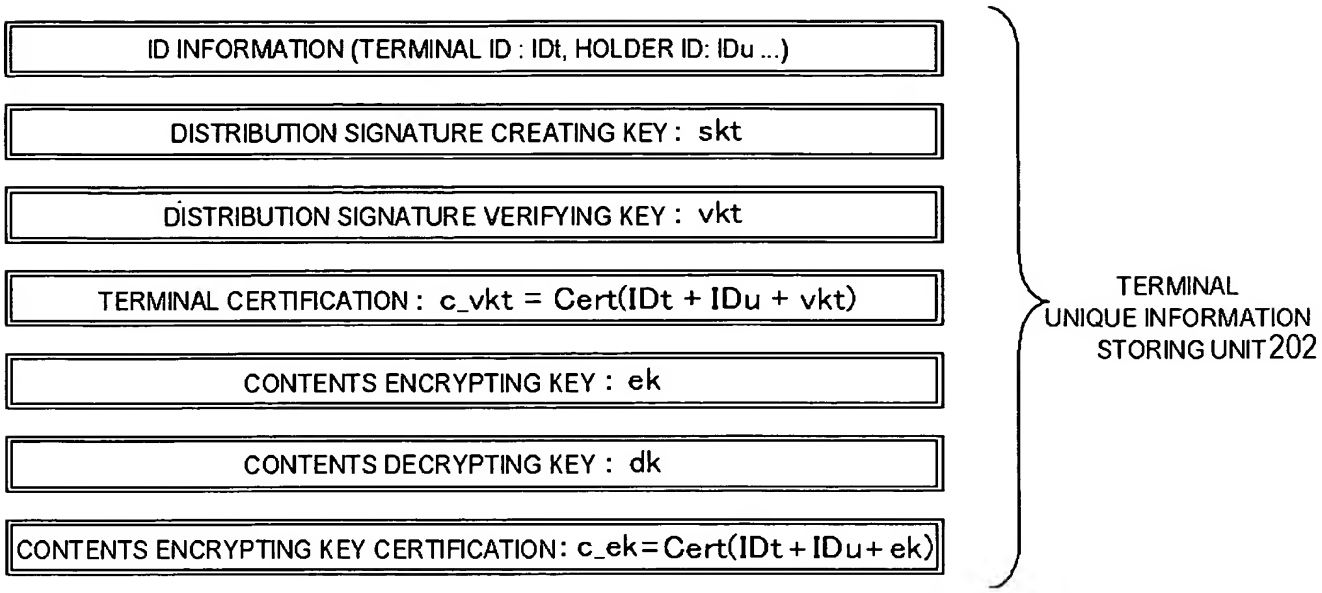
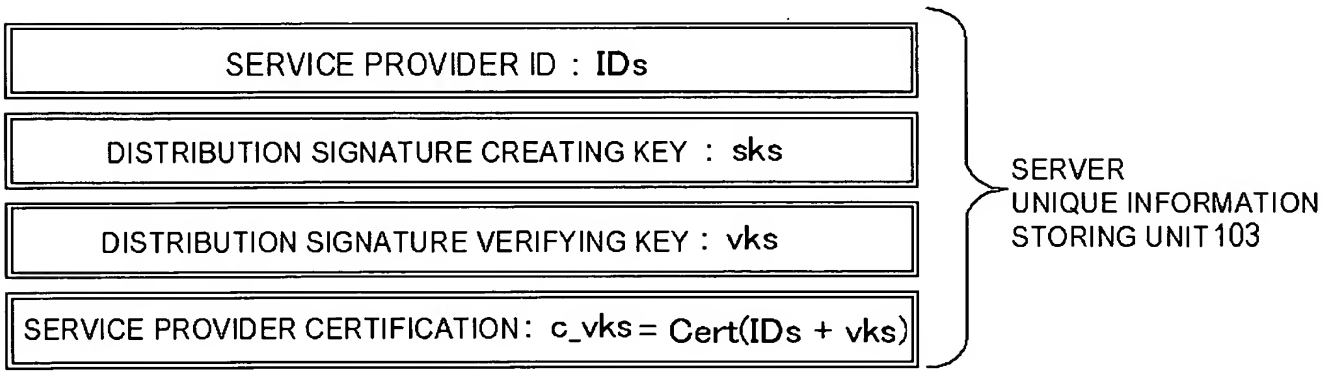


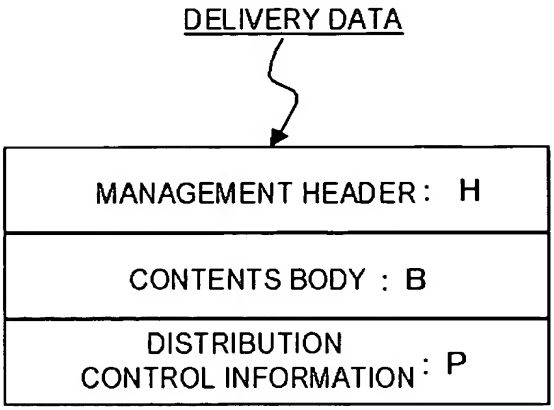
FIG. 5



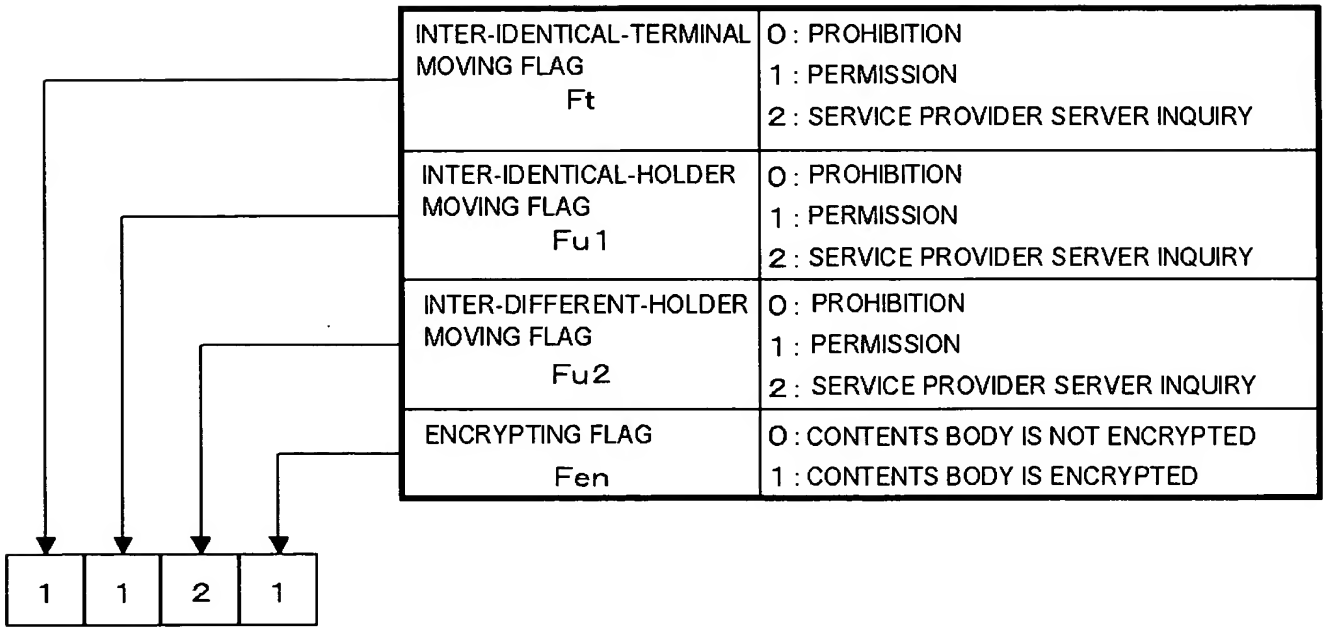
10/556068

FIG. 6

(A)



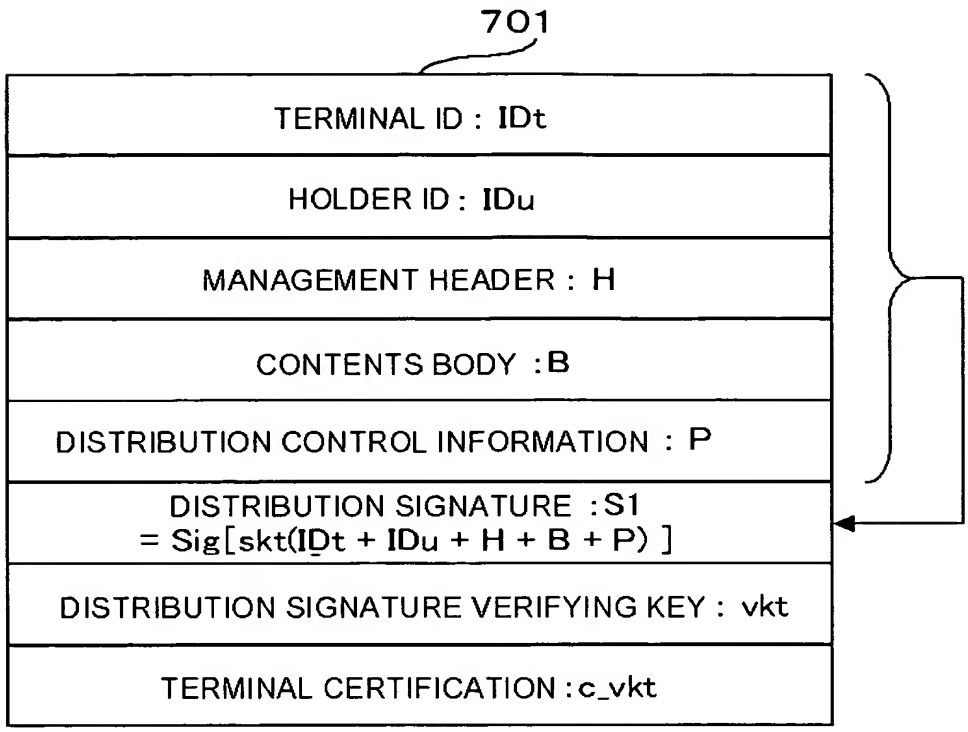
(B)



US 20050256968

FIG. 7

(A) SAFING DATA



(B) SAFING DATA DESIGNATED TO BE ENCRYPTED

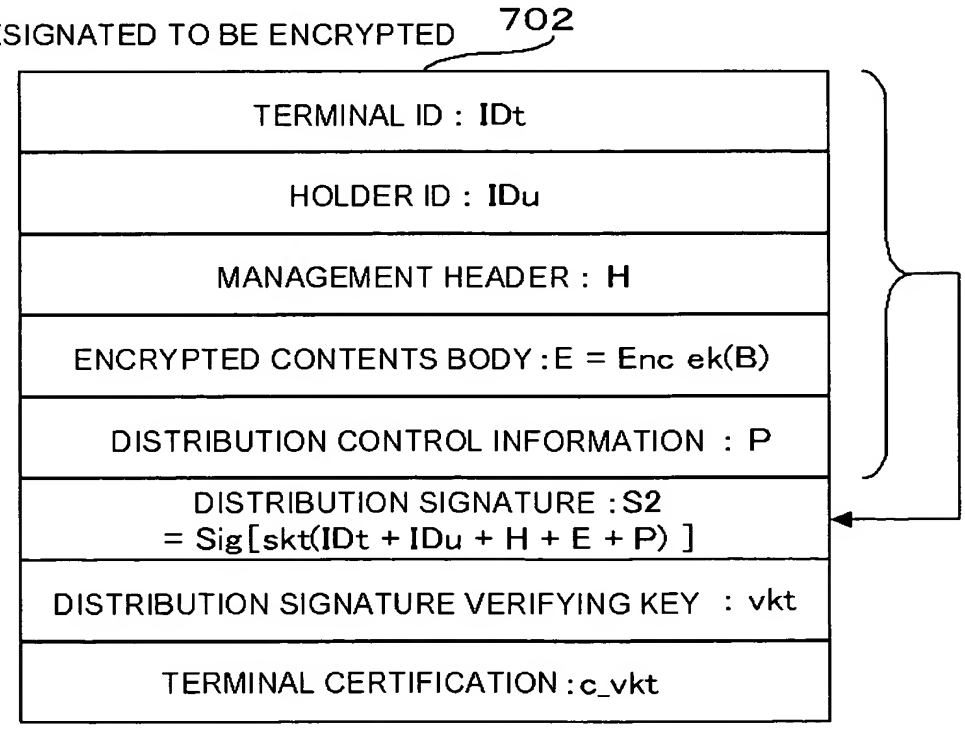


FIG. 8

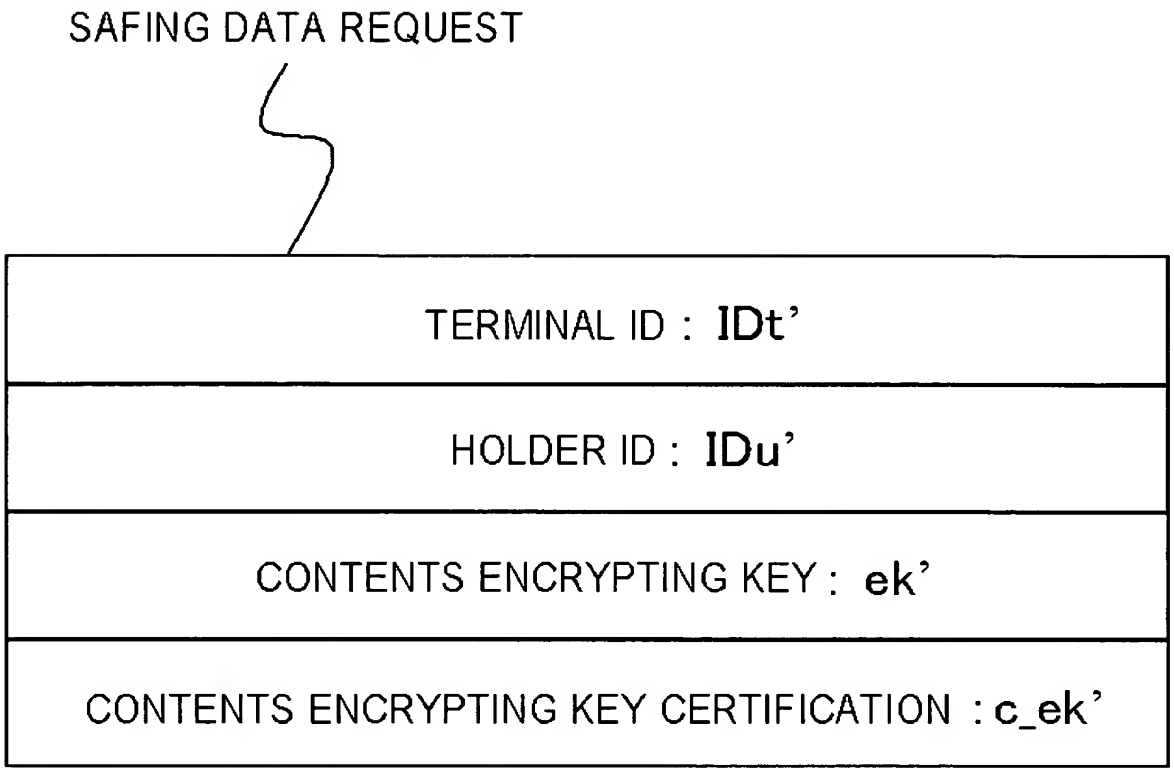
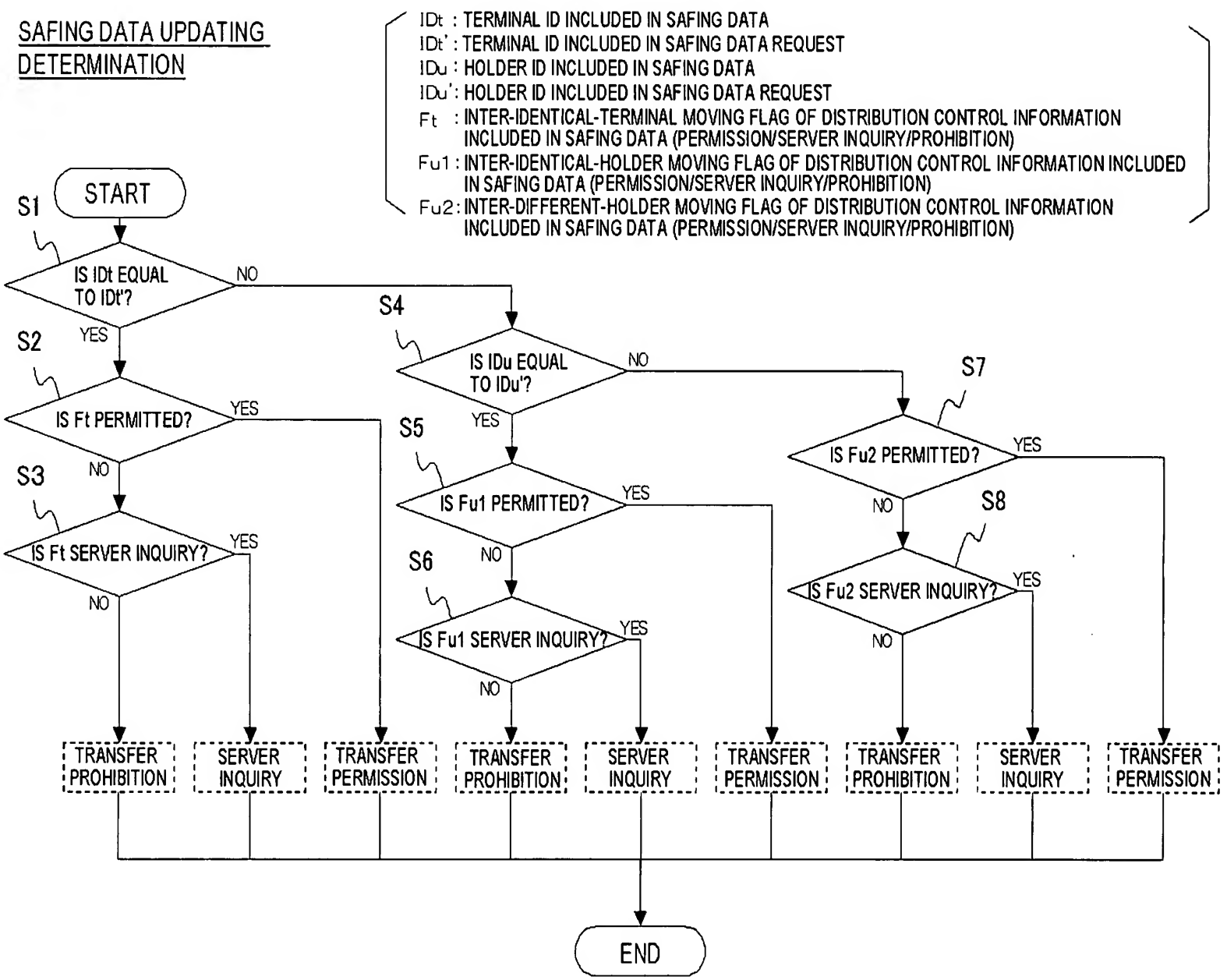

SAFING DATA REQUEST
TERMINAL ID : IDt'
HOLDER ID : IDu'
CONTENTS ENCRYPTING KEY : ek'
CONTENTS ENCRYPTING KEY CERTIFICATION : c_ek'

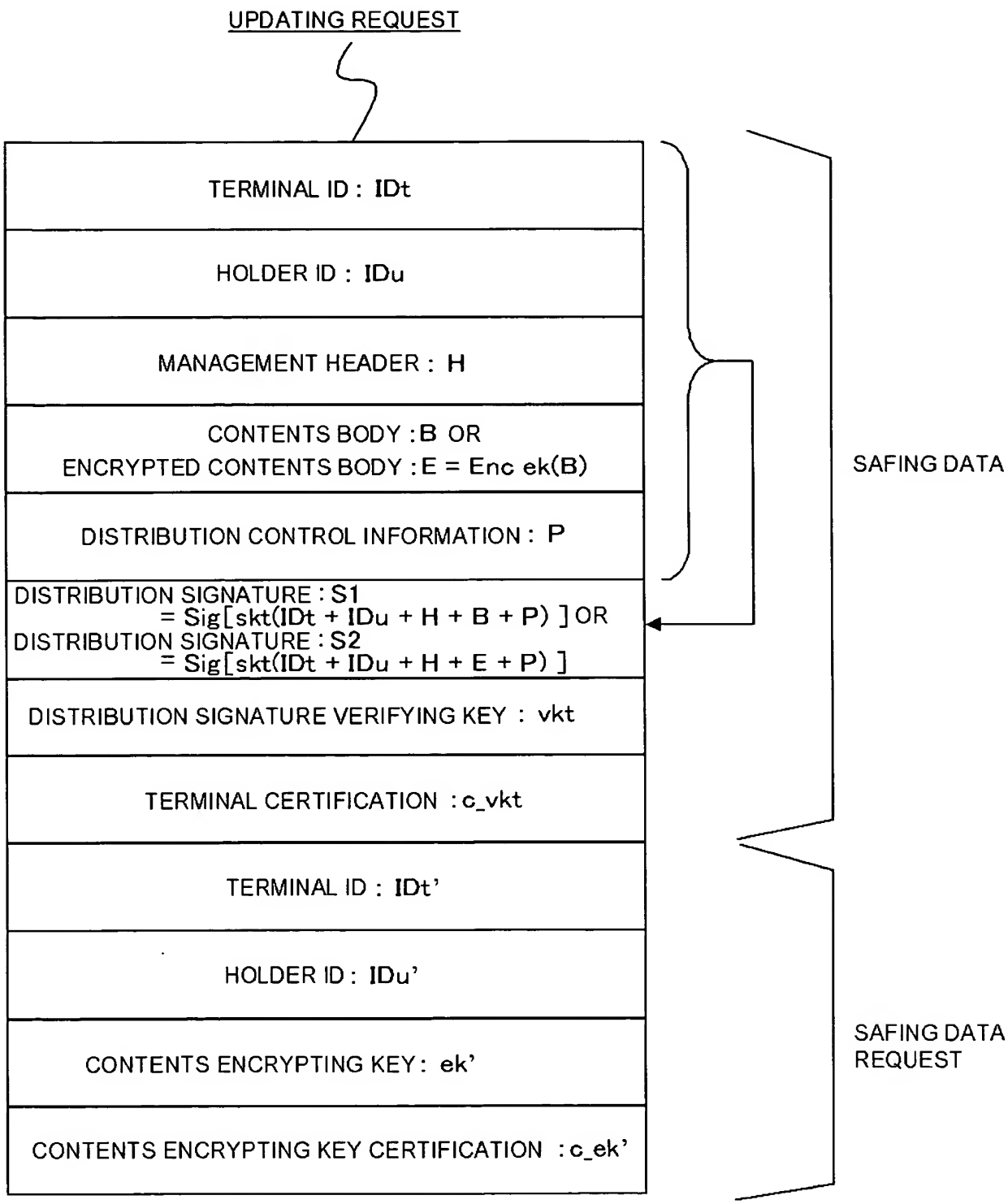
FIG. 9



Daigo TAGUCHI, et al.
DISTRIBUTION CONTROL METHOD AND DISTRIBUTION CONTROL SYSTEM FOR ...
Filed November 8, 2005
Atty. Docket No.: Q91332
SUGHRUE MION, PLLC: 202-293-7060
Sheet 8 of 22

10/556068

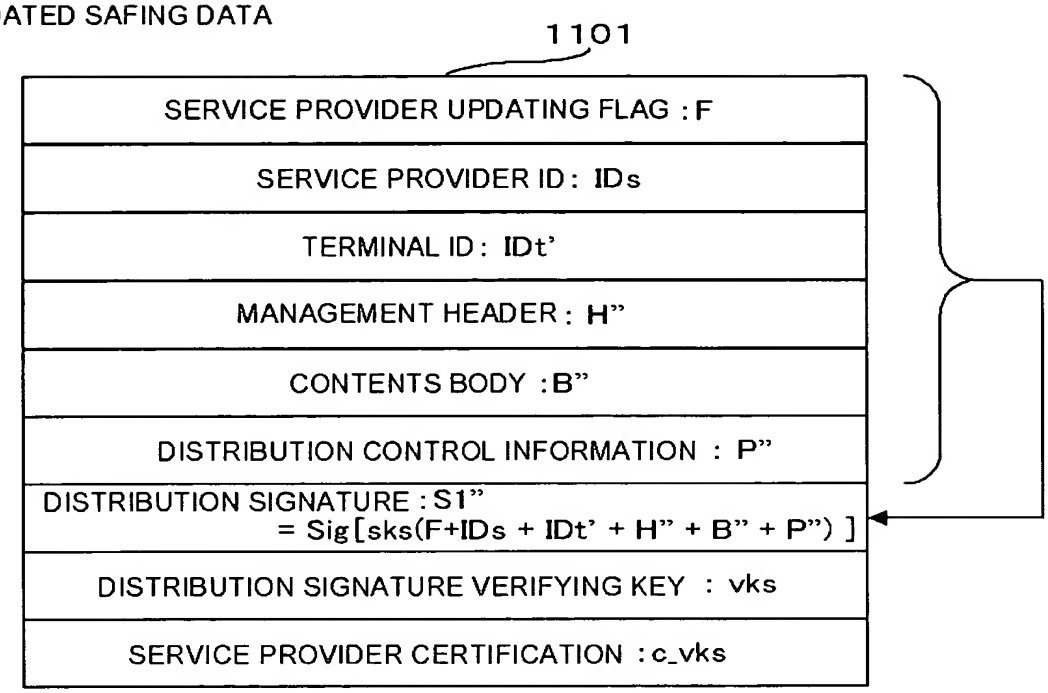
FIG. 10


UPDATING REQUEST
TERMINAL ID : IDt
HOLDER ID : IDu
MANAGEMENT HEADER : H
CONTENTS BODY : B OR
ENCRYPTED CONTENTS BODY : E = Enc ek(B)
DISTRIBUTION CONTROL INFORMATION : P
DISTRIBUTION SIGNATURE : S1
= Sig[skt(IDt + IDu + H + B + P)] OR
DISTRIBUTION SIGNATURE : S2
= Sig[skt(IDt + IDu + H + E + P)]
DISTRIBUTION SIGNATURE VERIFYING KEY : vkt
TERMINAL CERTIFICATION : c_vkt
TERMINAL ID : IDt'
HOLDER ID : IDu'
CONTENTS ENCRYPTING KEY : ek'
CONTENTS ENCRYPTING KEY CERTIFICATION : c_ek'
SAFING DATA
SAFING DATA REQUEST

US 20070356068

FIG. 11

(A) UPDATED SAFING DATA



(B) UPDATED SAFING DATA DESIGNATED TO BE ENCRYPTED

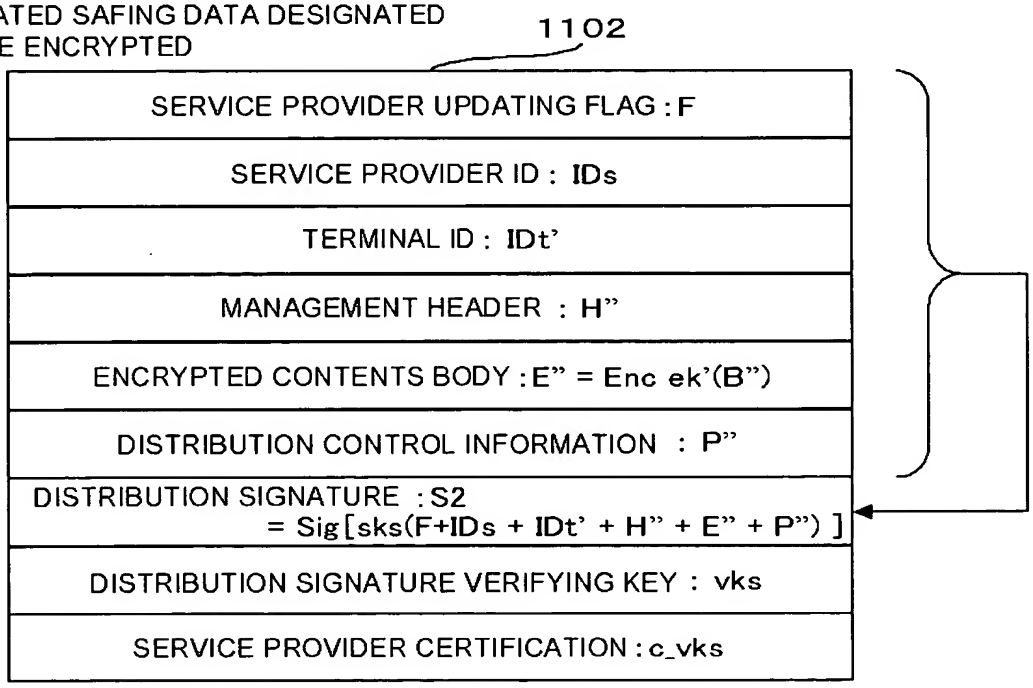
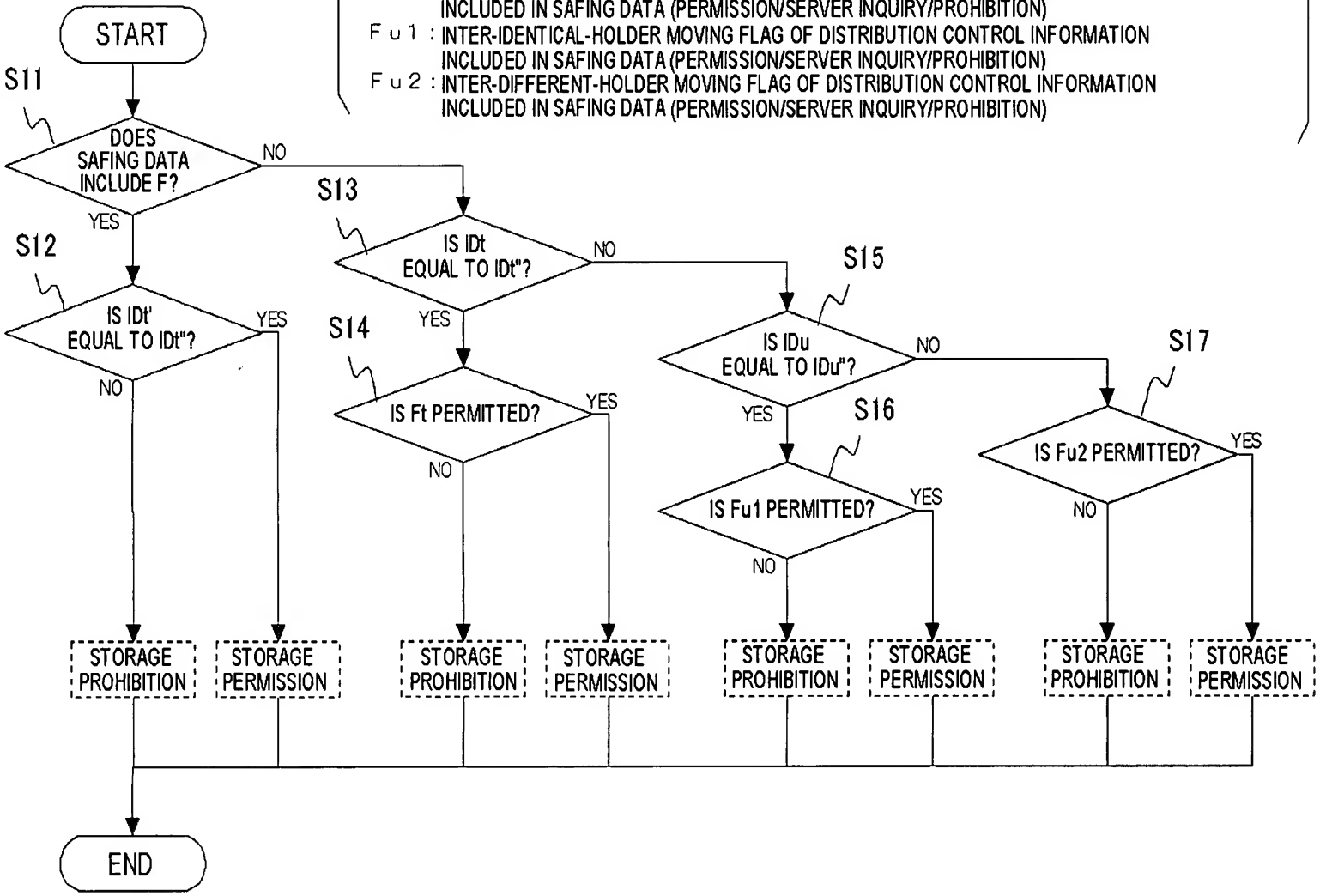


FIG. 12

DATA SAFETY CHECK

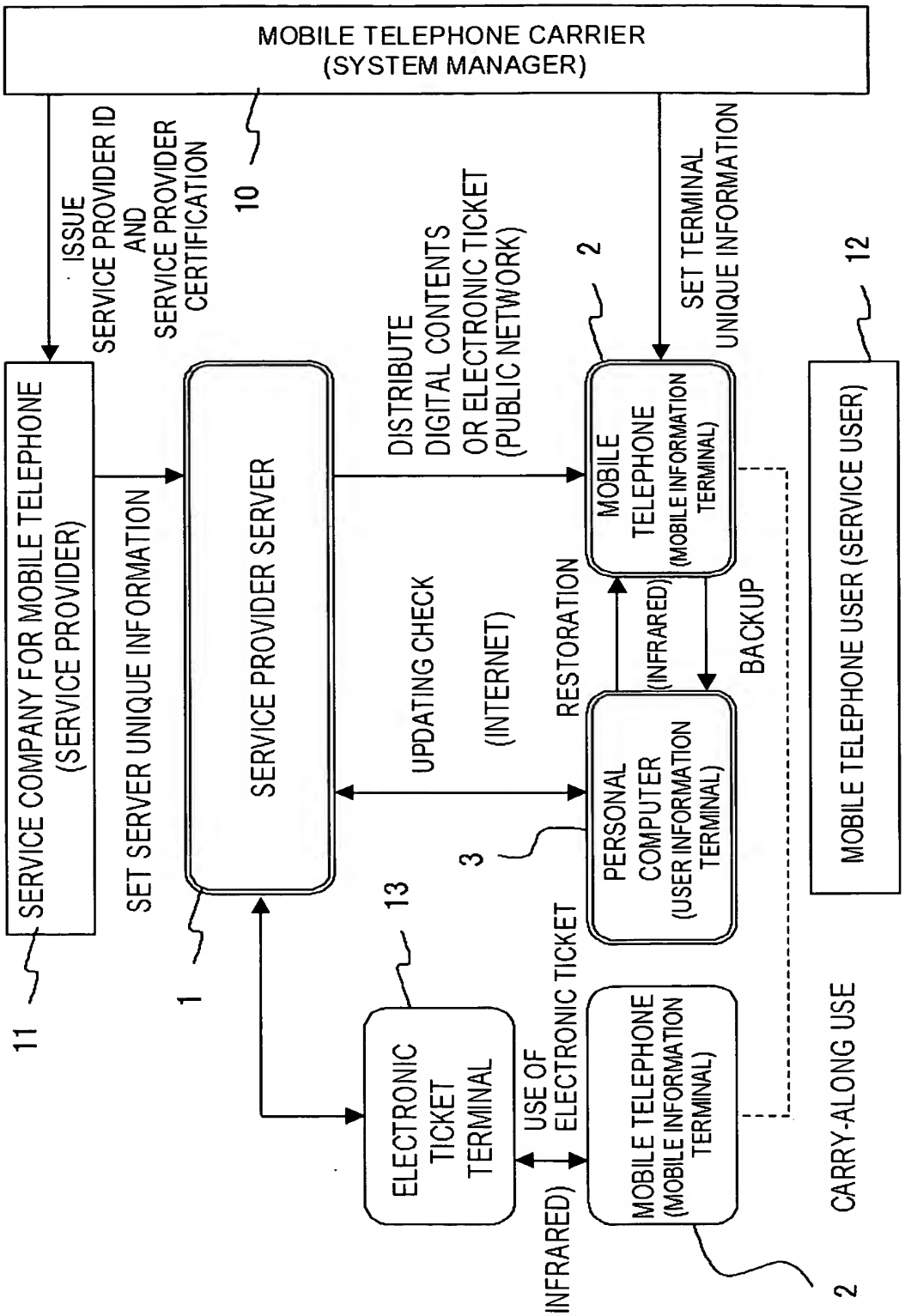
F : SERVICE PROVIDER UPDATING FLAG
IDt : TERMINAL ID INCLUDED IN SAFING DATA (UPDATING IS NOT PERFORMED BY SERVICE PROVIDER)
IDt' : TERMINAL ID INCLUDED IN SAFING DATA (UPDATING IS PERFORMED BY SERVICE PROVIDER)
IDt" : TERMINAL ID STORED IN MOBILE INFORMATION TERMINAL
IDu : HOLDER ID INCLUDED IN SAFING DATA
IDu" : HOLDER ID STORED IN MOBILE INFORMATION TERMINAL
Ft : INTER-IDENTICAL-TERMINAL MOVING FLAG OF DISTRIBUTION CONTROL INFORMATION INCLUDED IN SAFING DATA (PERMISSION/SERVER INQUIRY/PROHIBITION)
Fu1 : INTER-IDENTICAL-HOLDER MOVING FLAG OF DISTRIBUTION CONTROL INFORMATION INCLUDED IN SAFING DATA (PERMISSION/SERVER INQUIRY/PROHIBITION)
Fu2 : INTER-DIFFERENT-HOLDER MOVING FLAG OF DISTRIBUTION CONTROL INFORMATION INCLUDED IN SAFING DATA (PERMISSION/SERVER INQUIRY/PROHIBITION)



Daigo TAGUCHI, et al.
DISTRIBUTION CONTROL METHOD AND DISTRIBUTION CONTROL SYSTEM FOR ...
Filed November 8, 2005
Atty. Docket No.: Q91332
SUGHRUE MION, PLLC: 202-293-7060
Sheet 11 of 22
10/556068

10/556068

FIG. 13



10/556066

FIG. 14

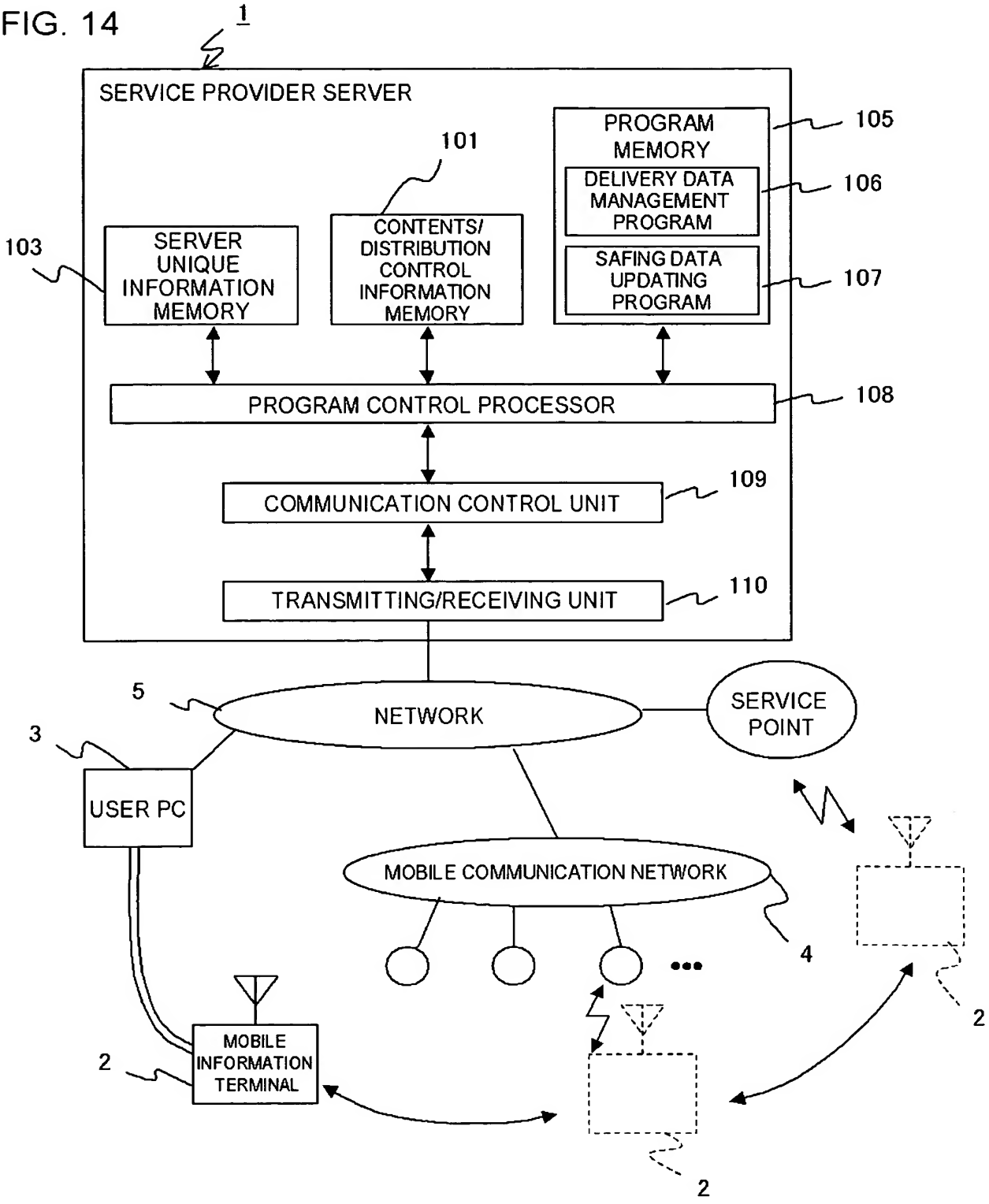
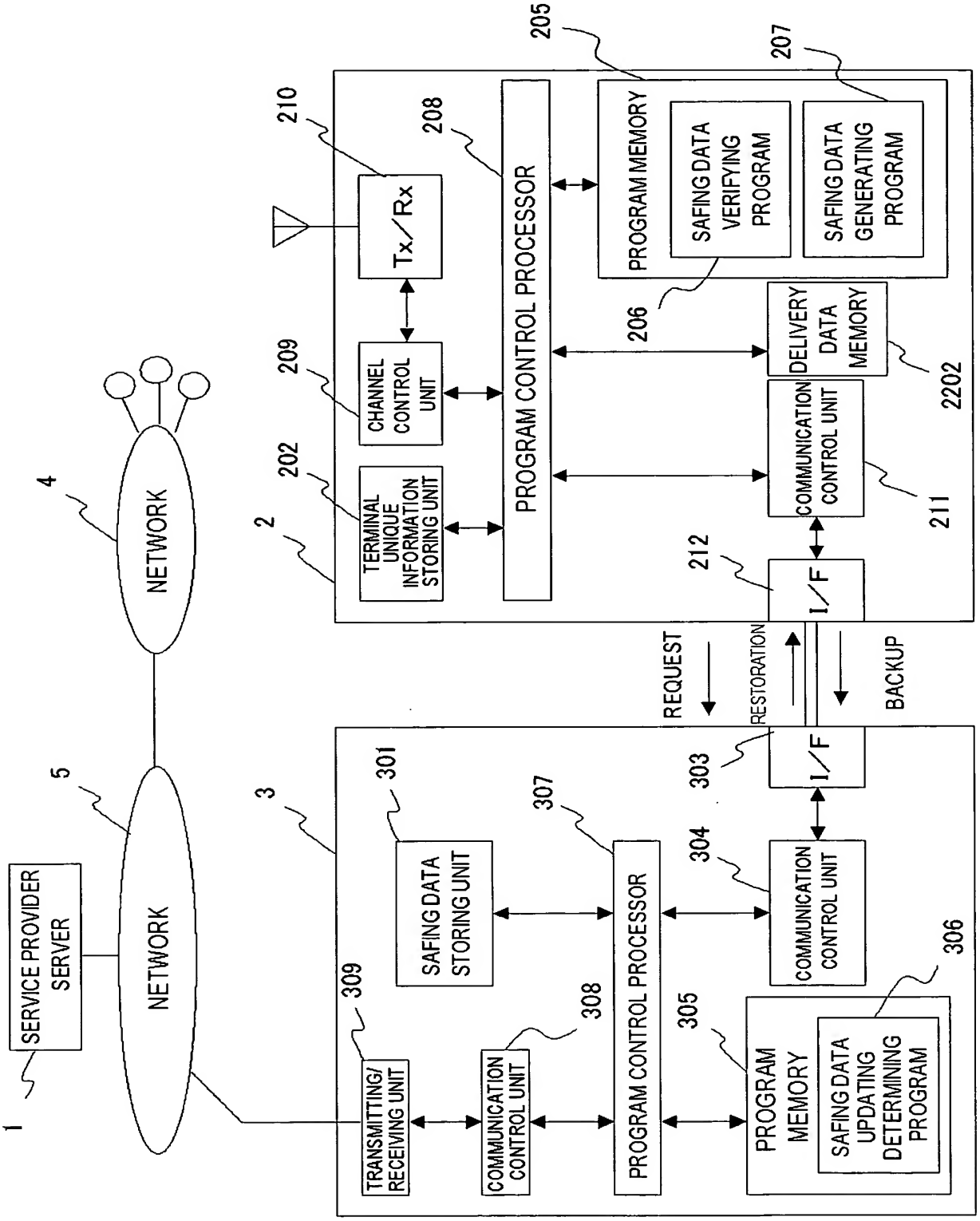
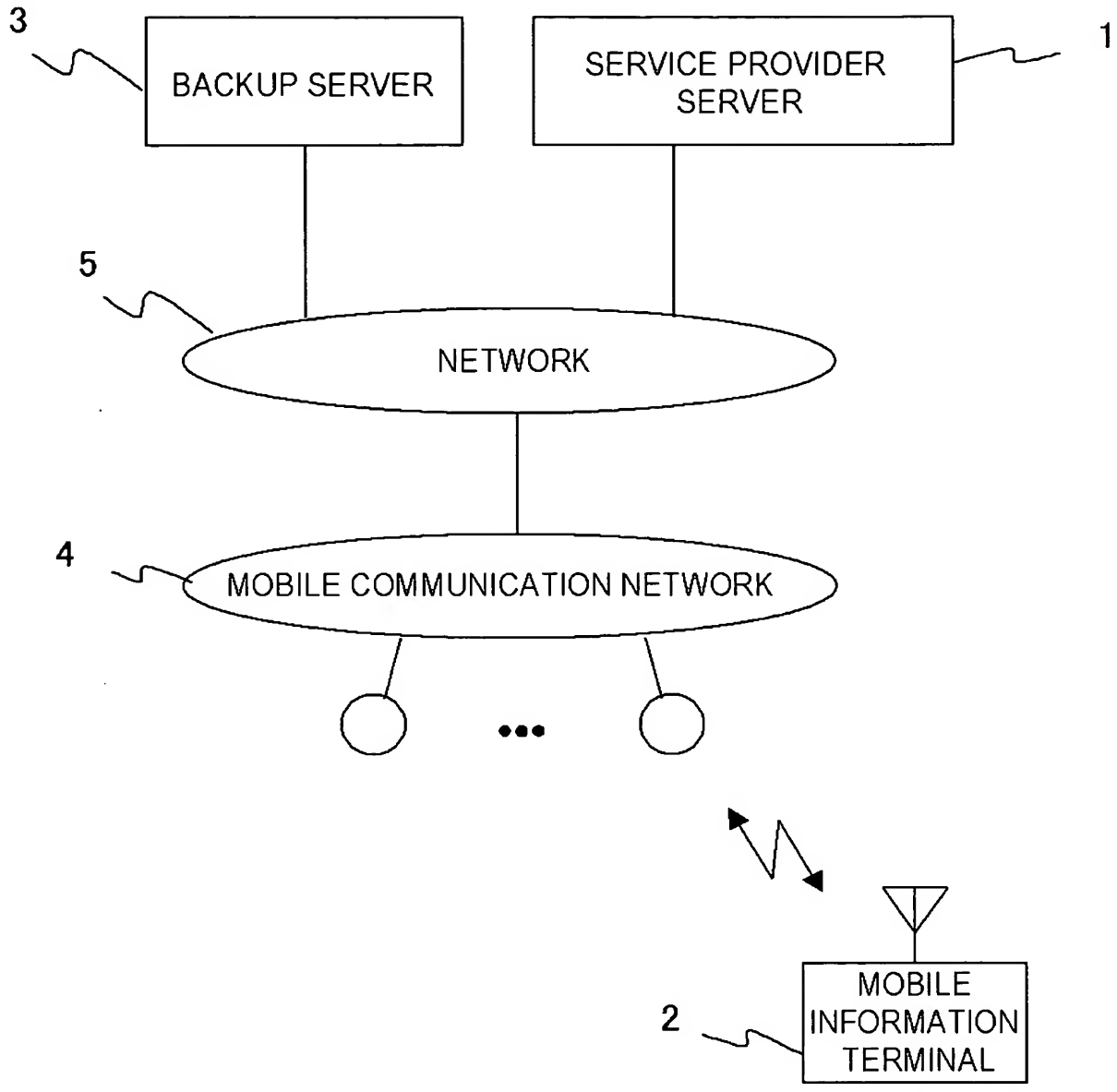


FIG. 15


1
SERVICE PROVIDER SERVER
5
NETWORK
4
NETWORK
2
3
TERMINAL UNIQUE INFORMATION STORING UNIT
202
CHANNEL CONTROL UNIT
209
Tx/Rx
210
PROGRAM CONTROL PROCESSOR
208
PROGRAM MEMORY
205
SAFING DATA VERIFYING PROGRAM
206
SAFING DATA GENERATING PROGRAM
207
DELIVERY DATA MEMORY
2202
COMMUNICATION CONTROL UNIT
211
I/F
212
REQUEST
RESTORATION
BACKUP
I/F
303
SAFING DATA STORING UNIT
301
PROGRAM CONTROL PROCESSOR
307
COMMUNICATION CONTROL UNIT
304
PROGRAM MEMORY
305
SAFING DATA UPDATING DETERMINING PROGRAM
306
TRANSMITTING/ RECEIVING UNIT
309
COMMUNICATION CONTROL UNIT
308

10/556068

FIG. 16



US 20/556068

FIG. 17

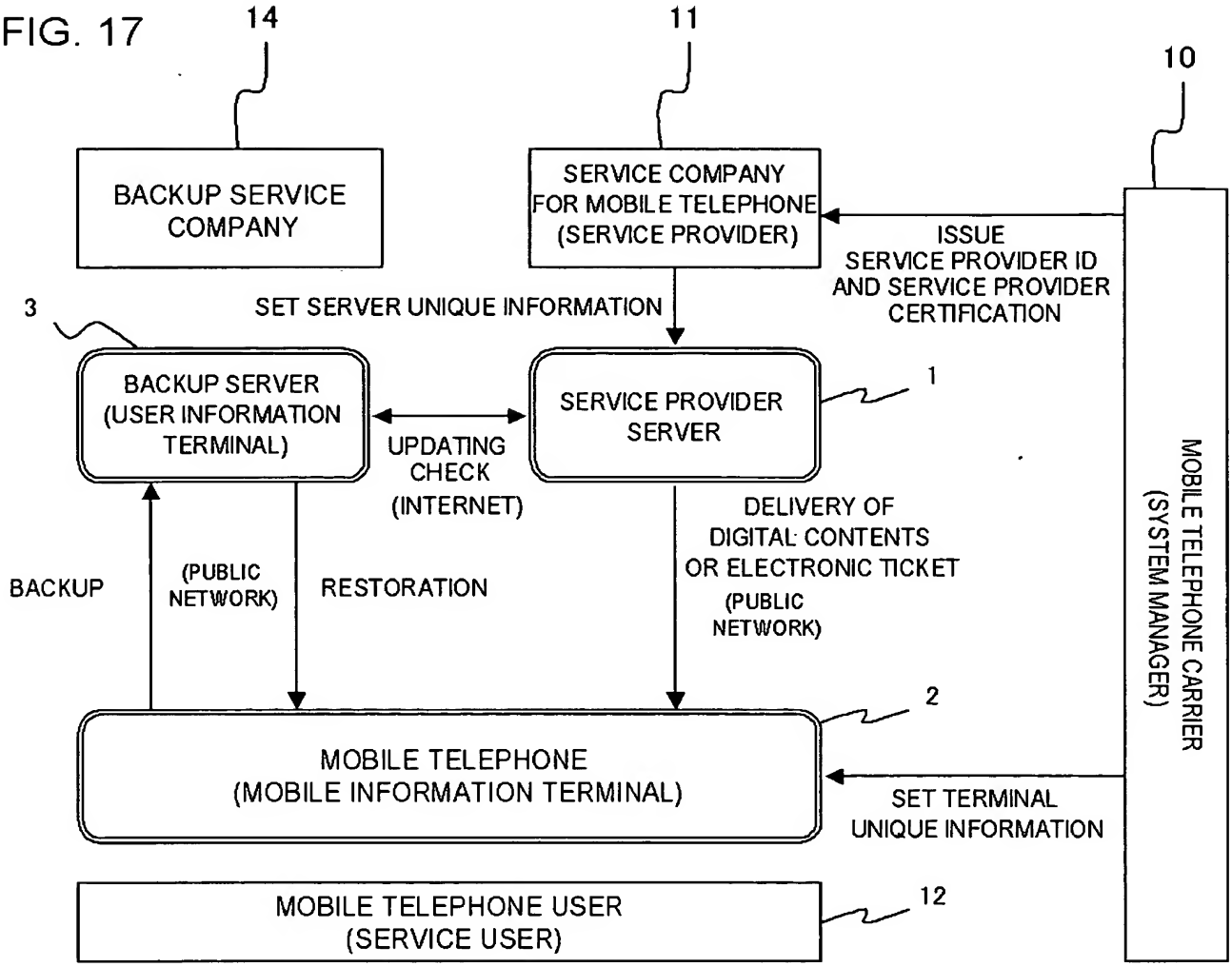


FIG. 18

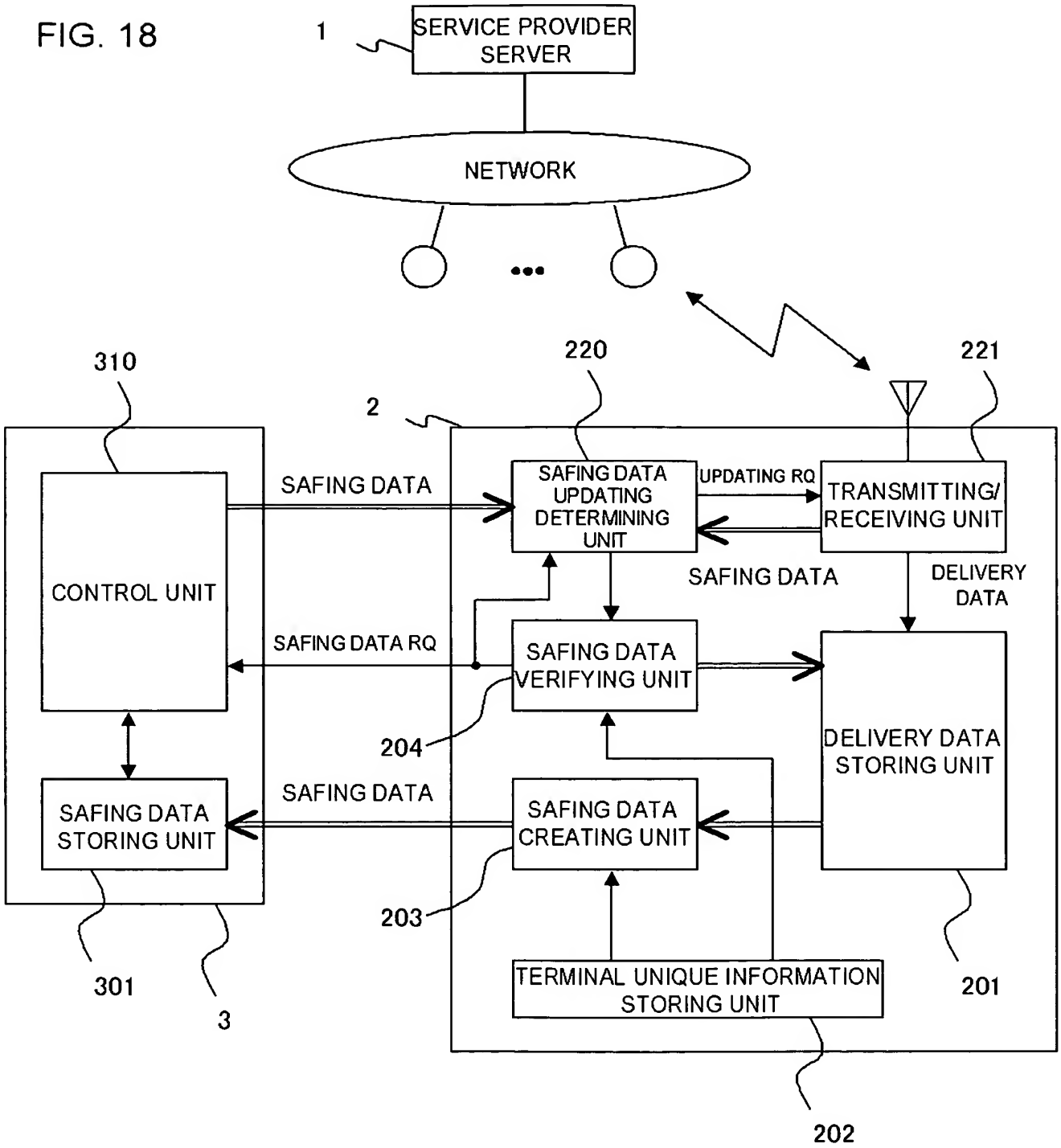

1
SERVICE PROVIDER SERVER
NETWORK
310
220
221
2
SAFING DATA
SAFING DATA UPDATING DETERMINING UNIT
UPDATING RQ
TRANSMITTING/ RECEIVING UNIT
CONTROL UNIT
SAFING DATA
DELIVERY DATA
SAFING DATA RQ
SAFING DATA VERIFYING UNIT
204
DELIVERY DATA STORING UNIT
SAFING DATA
SAFING DATA STORING UNIT
SAFING DATA
SAFING DATA CREATING UNIT
203
TERMINAL UNIQUE INFORMATION STORING UNIT
301
3
201
202

FIG. 19

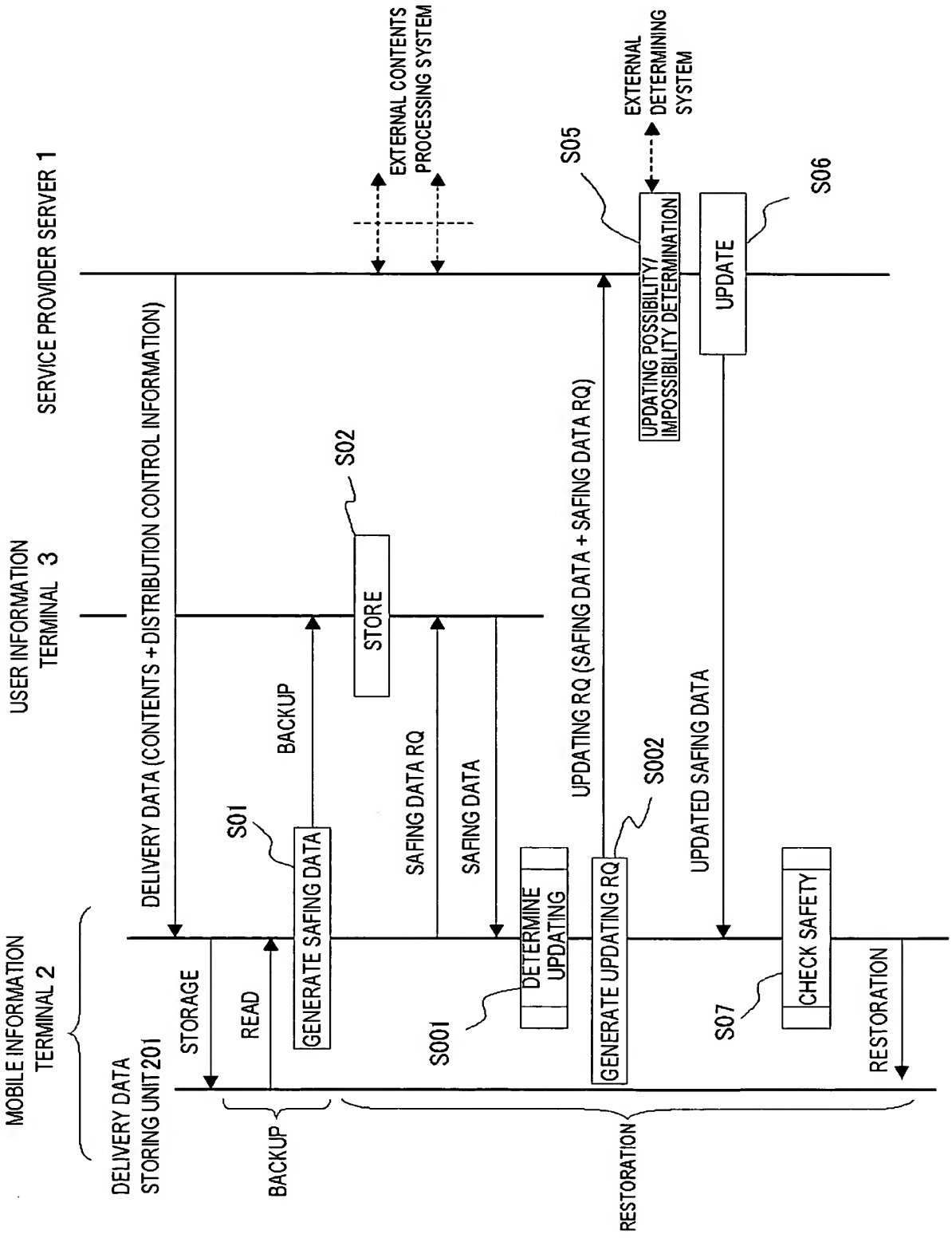
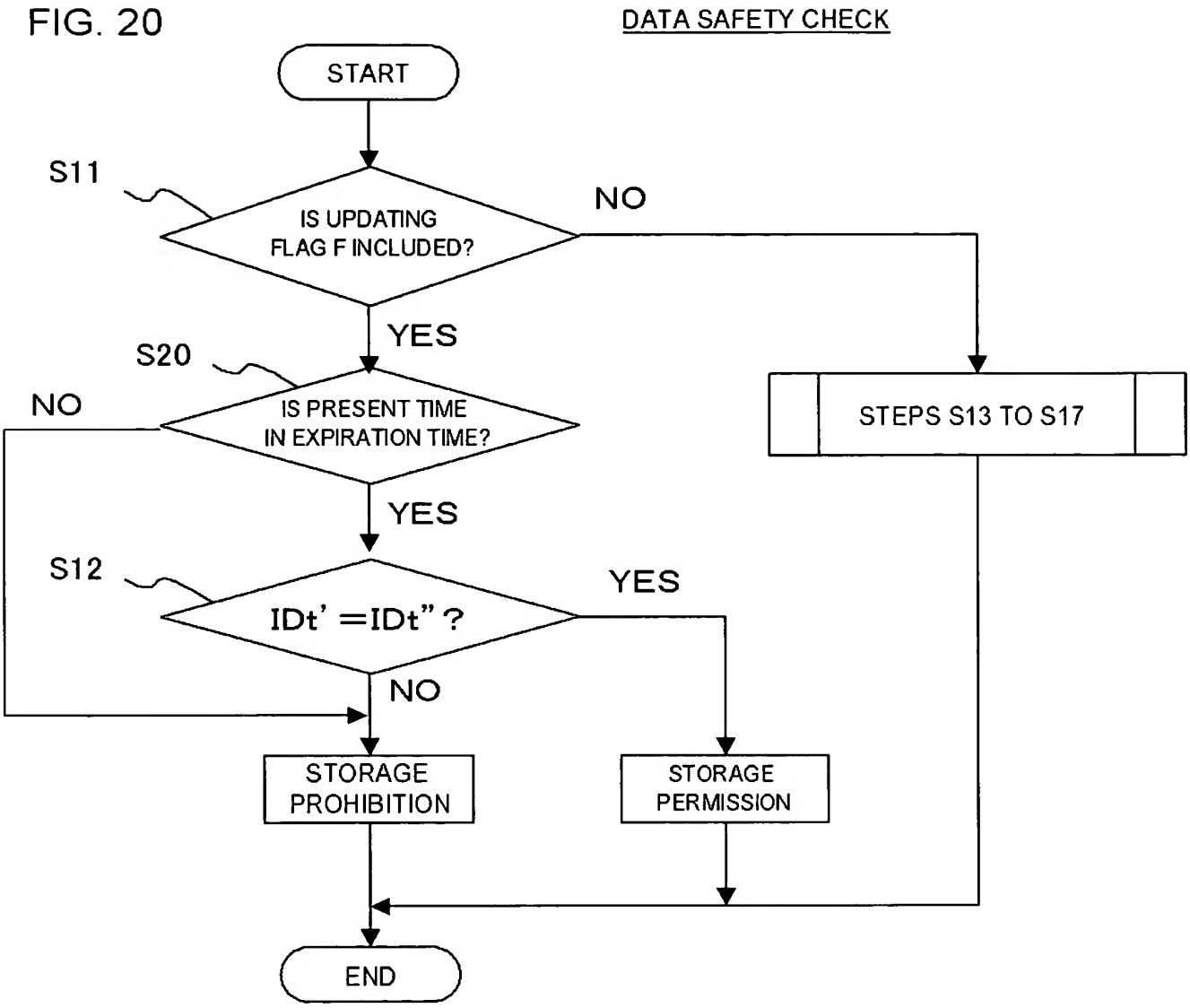

MOBILE INFORMATION TERMINAL 2
DELIVERY DATA STORING UNIT 201
USER INFORMATION TERMINAL 3
SERVICE PROVIDER SERVER 1
EXTERNAL CONTENTS PROCESSING SYSTEM
EXTERNAL DETERMINING SYSTEM
DELIVERY DATA (CONTENTS + DISTRIBUTION CONTROL INFORMATION)
STORAGE
READ
BACKUP
GENERATE SAFING DATA
S01
BACKUP
STORE
S02
SAFING DATA RQ
SAFING DATA
S001
DETERMINE UPDATING
UPDATING RQ (SAFING DATA + SAFING DATA RQ)
GENERATE UPDATING RQ
S002
UPDATING POSSIBILITY/ IMPOSSIBILITY DETERMINATION
S05
UPDATE
S06
UPDATED SAFING DATA
S07
CHECK SAFETY
RESTORATION
RESTORATION

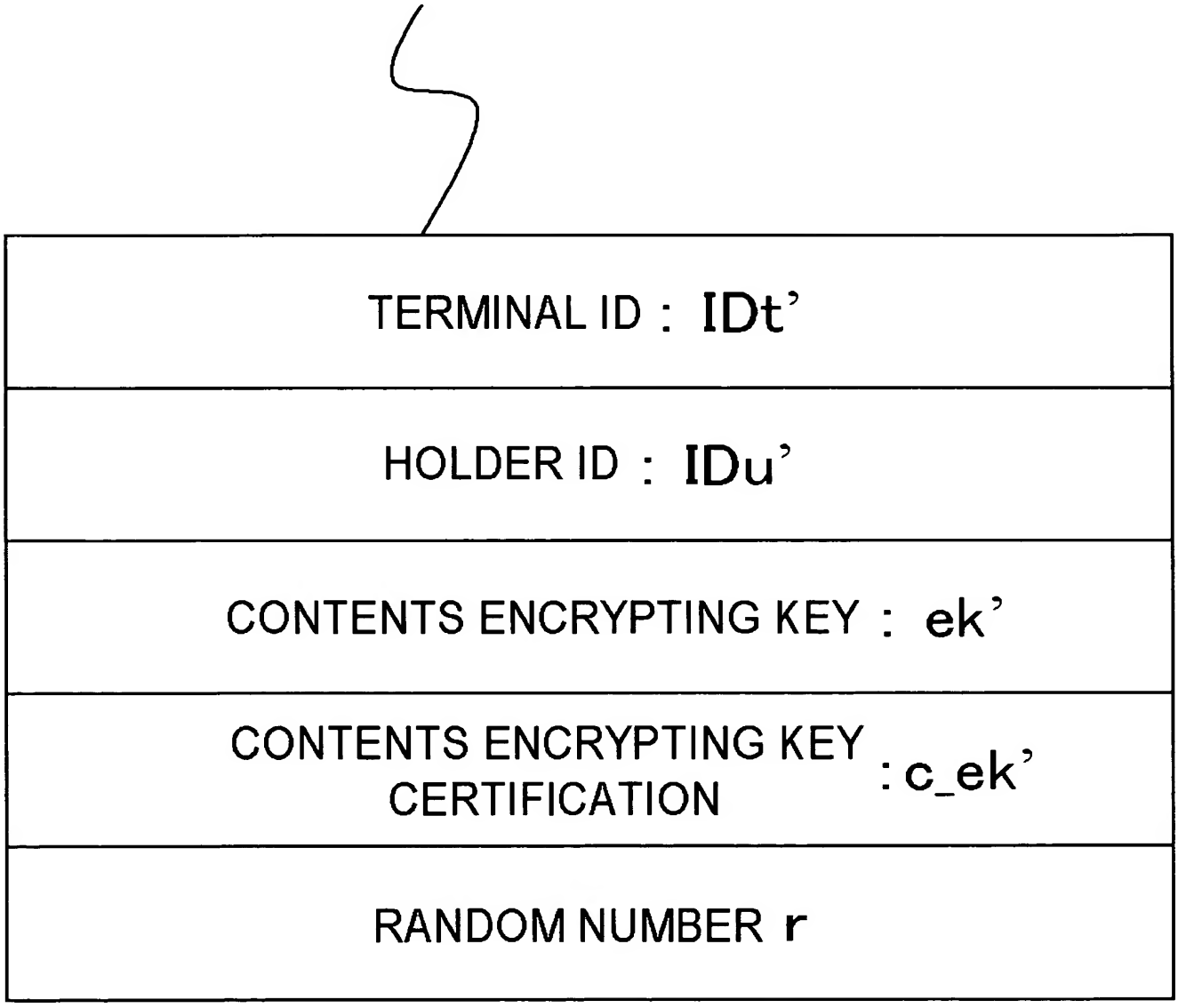
FIG. 20


DATA SAFETY CHECK
START
S11
IS UPDATING FLAG F INCLUDED?
NO
YES
S20
IS PRESENT TIME IN EXPIRATION TIME?
NO
YES
STEPS S13 TO S17
S12
IDt' =IDt" ?
YES
NO
STORAGE PROHIBITION
STORAGE PERMISSION
END

10/556068

FIG. 21

SAFING DATA REQUEST



10/556068

FIG. 22

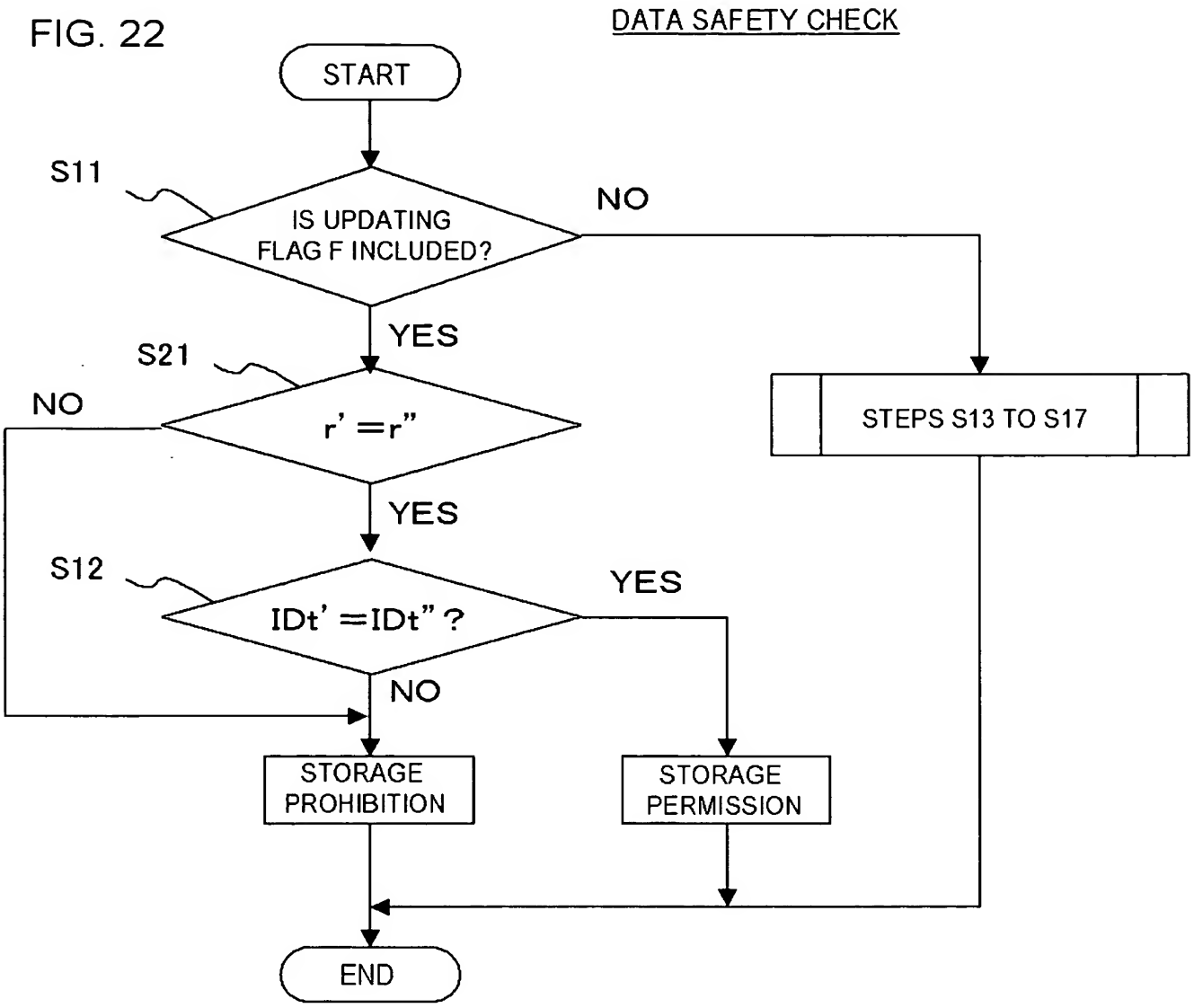


FIG. 23

```
enum RESULT {restoreDirect, restoreAfterServerUpdate, restoreFobiedden};

RESULT Check(          int terminal_id1,          int terminal_id2,
                       int user_id1,              int user_id2,          )
{
        // WHEN TERMINAL IDENTIFICATION INFORMATION IS IDENTICAL,
        // RESTORATION IS PERMITTED
        if  (terminal_id1 == terminal_id2)
                return restoreDirect;

        // WHEN RESTORATION DATE IS FEBRUARY 14, 2004, AND WHEN USER ID IS IDENTICAL,
        // RESTORATION IS PERMITTED AFTER SERVER INQUIRY
        char  currentDate[9];
        _strdate(currentDate);
        if  (strcmp (currentDate, "02/14/04") == 0 && user_id1 == user_id2 )
                return restoreAfterServerUpdate;

        //RESTORATION IS NOT PERMITTED
        return restoreFobidden;
}
```